

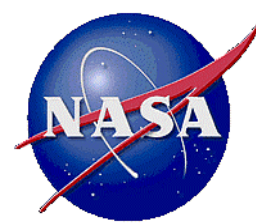
Need for Scenario-Based Accident Modeling

Leadership ViTS Meeting
January 03, 2005

Bryan O'Connor
Chief
Office of Safety and Mission Assurance

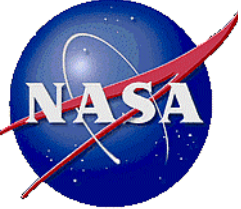
"Mission success stands on the foundation of our unwavering commitment to safety"

Administrator Sean O'Keefe, January 2003



Need to Identify Complex Accident Scenarios

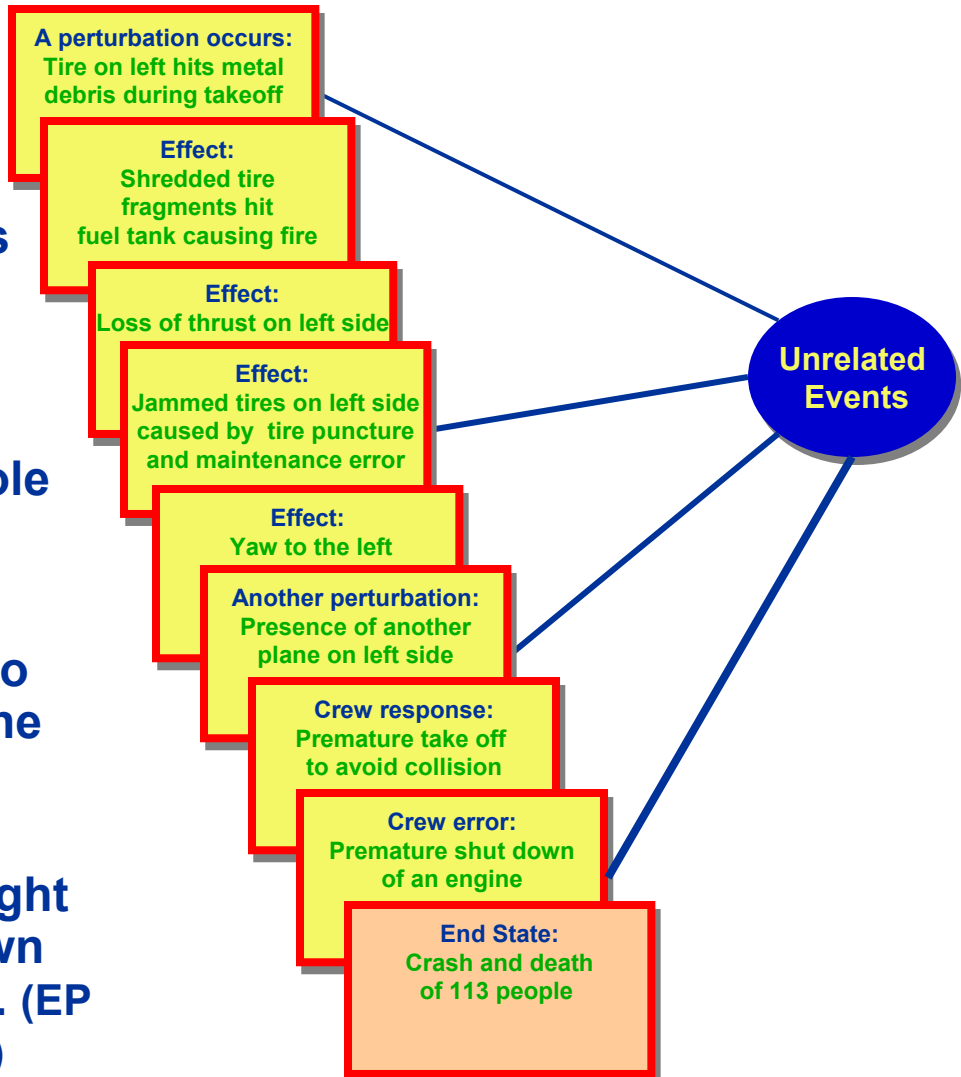
- Experience has shown that multiple, unrelated, and sometimes benign perturbations have challenged our systems in complex ways we would have never expected.
- High-consequence scenarios can emerge as a result of the occurrence of multiple unrelated events.
- Traditional system safety evaluations (e.g., FMEA) often model the response of the system to a single perturbation (failure or process deviation):
 - Accident scenarios predicted by these models tend to be incomplete.
 - From a risk management point of view, relying solely on such analyses, may cause relatively unimportant issues to receive excessive attention, while other important issues may go unidentified.

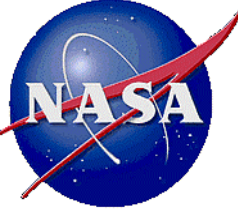


Crash of Air France Concorde in July 2000 Involved Multiple Events

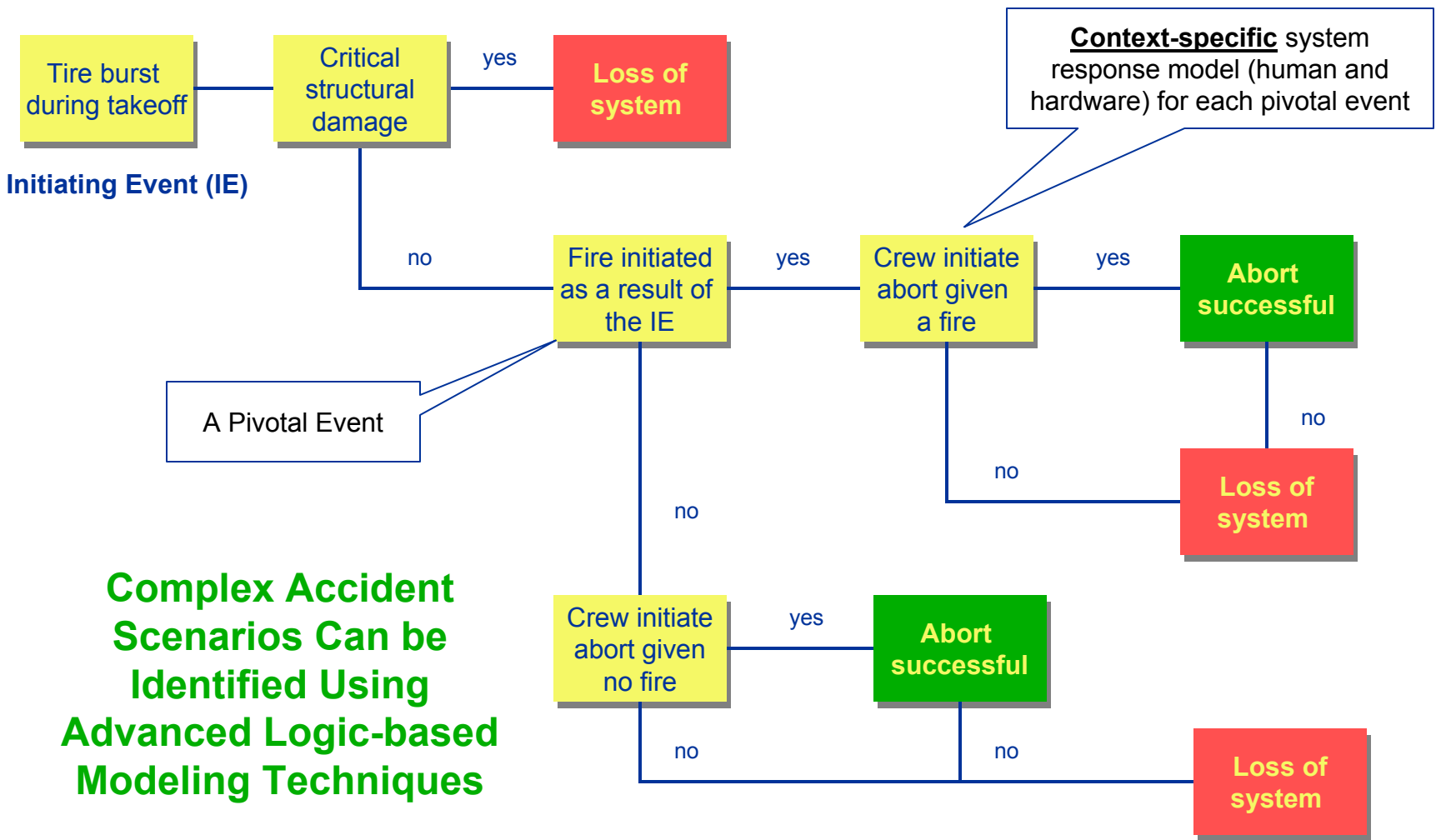


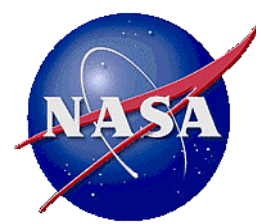
- Metal strip on runway punctures tires.
- Piece of tire comes free and punctures the fuel tank.
- Fuel pours out the punctured hole and ignites.
- Left tires jam.
- The pilot prematurely takes off to avoid collision with another plane waiting to cross Concorde's runway.
- At 25 feet off the ground, the Flight Engineer prematurely shuts down #2 engine which was not on fire. (EP specifies engine shutdown at 400 ft)





An Example of Event Sequence Diagram (ESD)





Conclusions

- Complex accidents scenarios can emerge as a result of combination of several unrelated mishap events
- A typical FMEA cannot identify complex scenarios such as the the one that led to the crash of the Concord.
- Identification of complex accident scenarios in safety assessment is both necessary and challenging.
- Application of systematic and logic-based safety assessment techniques, such as Event Sequence Diagrams, Event Trees, and Fault Trees, to accident scenario development and analysis is essential to predict complex mishap events
- **Effective risk management strategies cannot be devised without the knowledge of plausible accident scenarios.**